

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-130098
 (43)Date of publication of application : 25.05.1993

(51)Int.CI. H04L 9/06
 H04L 9/14
 G06F 15/30
 G06K 17/00
 G09C 1/00
 H04K 1/00

(21)Application number : 03-286348 (71)Applicant : HITACHI LTD
 (22)Date of filing : 31.10.1991 (72)Inventor : KANEKAWA NOBUYASU

(54) TRANSMISSION METHOD FOR CIPHERING DATA AND CARD WITH CIPHERING DATA RECORDED THEREON

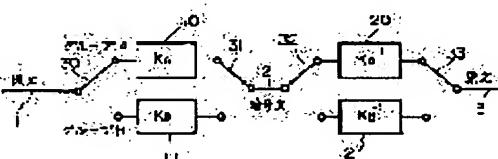
(57)Abstract:

PURPOSE: To preclude the possibility of ciphering from being decoded by a third party by using plural ciphering systems or ciphering keys depending on types of characters, codes and data used for an original text.

CONSTITUTION: Codes, characters and data with high frequency of appearance of an original text are classified into a group A and codes characters and data with low frequency of appearance are classified into a group B.

The codes characters and data classified into the group A are ciphered by a ciphering operation 10 employing the ciphering system or ciphering key KA corresponding to the group A and the codes characters and data classified into the group B are ciphered by a ciphering operation 11 employing the ciphering system or ciphering key KB corresponding to the group B and a ciphered text 2 is obtained. The ciphered text 2 is sent from a sender side to a receiver side through various transmission means. A ciphering decoding operation 20

(21) corresponding to each group at the receiver side is used to decode the ciphered text thereby obtaining an original text 3.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平5-130098

(43)公開日 平成5年(1993)5月25日

| | | | | |
|--------------------------|-------|---------|--------------------------|--------|
| (51)Int.Cl. ⁵ | 識別記号 | 序内整理番号 | F I | 技術表示箇所 |
| H 04 L 9/06 9/14 | | | | |
| G 06 F 15/30 | 3 4 0 | 6798-5L | | |
| G 06 K 17/00 | L | 8623-5L | | |
| | | 7117-5K | H 04 L 9/02 | Z |
| | | | 審査請求 未請求 請求項の数20(全 13 頁) | 最終頁に続く |

(21)出願番号 特願平3-286348

(22)出願日 平成3年(1991)10月31日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 金川 信康

茨城県日立市久慈町4026番地 株式会社日立製作所日立研究所内

(74)代理人 弁理士 鶴沼 辰之

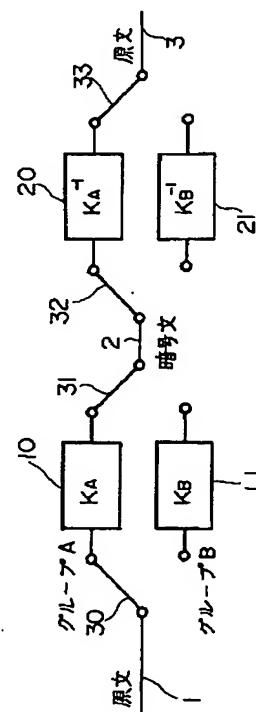
(54)【発明の名称】 暗号化データの伝送方法及び暗号化データが記録されたカード

(57)【要約】

【目的】 リモートセンシングデータ、有料の放送内容、コンピュータデータ、IDカードなどの特定の符号パターンの出現頻度が極端に高く、原文のパターンが容易に推定されやすく、暗号が解読されやすい用途での暗号化データの伝送方法を提供すること。

【構成】 原文において、出現頻度が高いパターン(符号)のグループと低いパターン(符号)グループとに分類し、それぞれのグループごとに別々の暗号化方式または、暗号化鍵を用いて暗号化する。

【効果】 本発明によれば、原文中の符号の出現頻度に関する知識や、原文の推定を手がかりにして、暗号が第三者に解読される畏れを少なくすることができる。



1

【特許請求の範囲】

【請求項1】 原文のデータを暗号化して伝送するデータ伝送方法であって、原文を構成する文字、符号、データの種別に応じて複数の暗号化方式または、暗号化鍵を使いわけることを特徴とする暗号化データの伝送方法。

【請求項2】 原文のデータを暗号化して伝送する暗号化データの伝送方法であって、暗号化データの送信側で原文において出現頻度が高いパターンが属するグループと出現頻度の低いパターン(符号)が属するグループとに分類し、それぞれのグループ毎に異なる暗号化方式または、暗号化鍵で原文を暗号化することを特徴とする暗号化データの伝送方法。

【請求項3】 DPCM方式でデータ圧縮を行つてデータ伝送を行う際に、DPCM方式の差分0を表す符号と差分0以外を表す符号とでは別個の暗号化方式または暗号化鍵を使用して暗号化することを特徴とする請求項1に記載の暗号化データの伝送方法。

【請求項4】 加入放送におけるテストパターンの映像信号と通常の放送番組の映像信号とでは別個の暗号化方式または暗号化鍵を使用して暗号化することを特徴とする請求項1に記載の暗号化データの伝送方法。

【請求項5】 コンピュータデータのうち\$FF、\$00、またはNOPを表す機械語に相当するデータとそれ以外のデータとでは別個の暗号化方式または暗号化鍵を使用して暗号化することを特徴とする請求項1に記載の暗号化データの伝送方法。

【請求項6】 キャッシュカードに各種データを記録し、記録された前記各種データを読み取るデータ伝送方法であつて、キャッシュカードの口座番号と暗証番号とでは別個の暗号化方式または暗号化鍵を使用して暗号化することを特徴とする請求項1に記載の暗号化データの伝送方法。

【請求項7】 IDカードを用いてIDカードに記録されたデータを送信する際にID番号と暗証番号とでは別個の暗号化方式または暗号化鍵を使用して暗号化してIDカードに記録することを特徴とする請求項1に記載の暗号化データの伝送方法。

【請求項8】 DPCM方式でデータ圧縮を行つてデータ伝送を行う際に、出現頻度が高いパターン(符号)のグループがDPCM方式の差分0を表す符号から構成され、出現頻度が低いパターン(符号)のグループがDPCM方式の差分0以外を表す符号から構成されることを特徴とする請求項2に記載の暗号化データの伝送方法。

【請求項9】 加入放送におけるデータ伝送であつて、出現頻度が高いパターン(符号)のグループが加入放送におけるテストパターンの映像信号から構成され、出現頻度が低いパターン(符号)グループが通常の放送番組の映像信号から構成されていることを特徴とする請求項2に記載の暗号化データの伝送方法。

【請求項10】 コンピュータデータを伝送する際に、

2

出現頻度が高いパターン(符号)のグループがコンピュータデータのうち\$FF、\$00、またはNOPを表す機械語から構成され、出現頻度が低いパターン(符号)グループがそれ以外のデータから構成されていることを特徴とする請求項2に記載の暗号化データの伝送方法。

【請求項11】 キャッシュカードに各種データを記録し、記録された前記各種データを読み取るデータ伝送方法であつて、出現頻度が高いパターン(符号)のグループがキャッシュカードの口座番号から構成され、出現頻度が低いパターン(符号)のグループが暗証番号から構成されていることを特徴とする請求項2に記載の暗号化データの伝送方法。

【請求項12】 出現頻度が高いパターン(符号)のグループがIDカードのID番号から構成され、出現頻度が低いパターン(符号)のグループが暗証番号から構成されていることを特徴とする請求項2に記載の暗号化データの伝送方法。

【請求項13】 原文を暗号化して伝送する暗号化データの伝送方法であつて、原文において出現頻度が高いパターンが属する第1のグループと、出現頻度が低いパターンが属する第2のグループとに分類し、これら各グループに対して相互に異なる暗号化方式または暗号化鍵を割り当てると共に、第1、第2のグループについて相互に異なる暗号化方式または暗号化鍵で暗号化された際に第2のグループに属する暗号文のパターンが第1のグループの暗号文のパターンと同一になる第2のグループの原文のパターンに対して第1、第2のグループとは異なる暗号化方式または暗号化鍵を割り当てて原文を暗号化することを特徴とする請求項2に記載の暗号化データの伝送方法。

【請求項14】 暗号化されたデータを伝送する暗号化データ伝送システムにおいて、原文と原文のうち出現頻度の高い第1のグループに属するパターン群とを比較し、一致するか否かを判定する第1の比較器群と、前記原文と原文のうち出現頻度の低い第2のグループに属するパターン群とを比較し、一致するか否かを判定する第2の比較器群と、

前記第1の比較器群の出力信号の論理和をとる第1の論理和演算手段と、

前記第2の比較器群の出力信号の論理和をとる第2の論理和演算手段と、

前記第1、第2の論理和演算手段の出力信号を取り込み負論理の論理積をとる論理積演算手段とを有し、前記第1、第2の論理和演算手段及び論理積演算手段の出力信号に基づいて前記原文のパターンをグループ分けすることを特徴とする暗号化データ伝送システムのグループ判別装置。

【請求項15】 暗号化されたデータを伝送する暗号化データ伝送システムにおいて、原文の出現頻度に応じて所定の暗号化方式または暗号化

50

鍵を用いて暗号化された暗号文と原文において出現頻度の高い第1のグループに属する原文のパターン群に対応する暗号文のパターン群とを比較し一致するか否かを判定する第1の比較器群と、

前記暗号文と原文において出現頻度の低い第2のグループに属する原文のパターン群に対応する暗号文のパターン群とを比較し、一致するか否かを判定する第2の比較器群と、

前記第1の比較器群の出力信号の論理和をとる第1の論理和演算手段と、

前記第2の比較器群の出力信号の論理和をとる第2の論理和演算手段と、

前記第1、第2の論理和演算手段の出力信号を取り込み負論理の論理積をとる論理積演算手段とを有し、前記第1、第2の論理和演算手段及び論理積演算手段の出力信号に基づいて前記暗号文のパターンを原文に対応してグループ分けすることを特徴とする暗号化データ伝送システムのグループ判別装置。

【請求項16】 DPCM方式でデータ圧縮を行ってデータを伝送する圧縮化データの伝送方法であって、DPCM方式の差分0を表す符号と差分0以外を表す符号とでは別個の暗号化方式または暗号化鍵を使用して暗号化することを特徴とする圧縮化データの伝送方法。

【請求項17】 加入放送におけるテストパターンの映像信号と通常の放送番組の映像信号とでは別個の暗号化方式または暗号化鍵を使用してスクランブリングすることを特徴とする加入放送番組のスクランブリング方法。

【請求項18】 コンピュータデータのうち\$FF、\$00、またはNOPを表す機械語に相当するデータとそれ以外のデータとでは別個の暗号化方式または暗号化鍵を使用して暗号化することを特徴とするコンピュータデータの伝送方法。

【請求項19】 キャッシュカードの口座番号と暗証番号とでは別個の暗号化方式または暗号化鍵を使用して暗号化して記録されまたは、別個の記録方式を用いて記録されたことを特徴とするキャッシュカード。

【請求項20】 IDカードのID番号と暗証番号とでは別個の暗号化方式または暗号化鍵を使用して暗号化して記録されまたは、別個の記録方式を用いて記録されたことを特徴とするIDカード。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、暗号化されたデータの伝送の方法に係り、特に解読されにくい（暗号強度の高い）暗号化データの伝送方法及び暗号化データが記録されたカードに関する。

【0002】

【従来の技術】従来から通信の秘密を確保するために、通信文を暗号化して伝送することが行なわれてきた。とくに近年では、コンピュータシステムの普及に伴う情報

化が進み、コンピュータ間を結ぶネットワークや、通信路での情報の漏洩が問題となる。

【0003】文献（松井 甲子雄著「コンピュータのための暗号組立法入門、森北出版株式会社（1986）によると暗号化の方法には大きく分けて、原文の文字系列の順序を入れ替える「転置式暗号」、原文の文字を他の文字に置き換える「換字式暗号」に分けられる。また、暗号の強度を増すために、これらを組み合わせる「混合式暗号」が広く用いられている。

【0004】「混合式暗号」のうち米国で標準化された暗号化規格の一つに「DES（Data Encryption Standard）暗号」がある。この方法は、上記文献 p.p. 94-105 に示すように 64 ビットを 1 ブロックとしたデータを 16 段にわたって転置と換字を繰り返すものである。

【0005】また原文中の文字の出現度数の分布が暗号解読の手掛かりとなるのを防ぐために、原文中の文字の出現度数分布を隠匿する「隠匿度数暗号」と呼ばれるものもある。この方法は、出現頻度の高い文字を出現頻度に合わせて複数の暗号文の文字に変換する方式で、原文の文字の出現頻度が暗号文の文字の出現頻度に反映しない特徴がある。

【0006】

【発明が解決しようとする課題】従来から用いられていた「DES 暗号」は、64 ビットを 1 ブロックとして処理をするために、原文がブロック単位で同一のパターンである場合には暗号文もブロック単位で同一のパターンとなる。従って以下に示すような用途に用いる場合は、原文と暗号文のブロックごとの出現度数の関連から暗号解読の手掛かりを第三者に与えるおそれがある。

【0007】また、「DES 暗号」に代表される混合式暗号は、複数の暗号化手段を組み合わせても原文の出現頻度が暗号文の出現頻度に伝搬する短所がある。

【0008】従来から用いられている「隠匿度数暗号」は、原文の文字の出現頻度が暗号文の文字の出現頻度に反映しないように考慮した暗号化方式で、原文の内容の推定を困難にすることにより、第三者に暗号解読の手掛かりを与えないようにしている。この方法は、人間が日常読み書きする文書を暗号化するのには十分な暗号強度をもっている。しかし、近年急激に普及したコンピュータなどへの使用について、十分な考慮がされていなかった。

【0009】暗号の隠匿性を守るためにには、暗号化の方式すなわち「鍵」の隠匿性の保護はもとより、原文の内容の隠匿性も必要である。原文の内容が容易に推定可能な場合には、第三者に暗号解読の手がかりを与えることになる。以下に示すような用途では、原文の内容が容易に推定されやすい。

【0010】遠隔地での計測値を伝送するリモートセンシングでは、通常データの差分をとりだしてデータを圧

縮して伝送する際にデータの差分のみを伝送するDPC M (Differential Pulse Code Modulation) 方式と呼ばれる方法がとられる。この場合、差分0を表す符号の出現頻度が極めて高い。

【0011】有料の衛星放送などの加入放送では、加入者以外には放送番組が視聴できないように放送内容を暗号化（スクランブリング）し、加入者のみにスクランブリングした信号を解読するデコーダを配布することが多い。しかし、通常放送だけでなく、テストパターンまでスクランブリングして送出すると、テストパターンの規則性からスクランブリングされた信号解読の手がかりを第三者に与えることになる。

【0012】コンピュータで扱うデータには、いわゆる人間が日常読み書きする文書の他に、プログラムや数値データなどの多様なデータが含まれている。

【0013】これらのうち機械語によるプログラムには、\$00や\$FF（\$は16進数を示す。）、そしてNOP（Non Operation）命令に相当する符号が極めて高い頻度で出現する。これらの出現頻度は、人間が日常読み書きする英語の文書で最も出現頻度の高いとされている文字“E”的出現頻度とは比較にならないほどである。

【0014】仮りに\$00や\$FFの符号が他の符号の10倍の出現頻度をもつとすると、出現頻度を隠匿するためにそれぞれに10種類の暗号の符号を割り当たなければならぬ。このように出現頻度の高い1つの原文の符号に複数の暗号文の符号を割り当てるためには、本例のように原文の符号の数と暗号文の符号の数とが256個と同数である場合には、逆に出現頻度の低い複数の原文の符号に1つの暗号文の符号を割り当てなければならない。従って暗号を解読するに当って、暗号文に対して一義的に原文が対応しない。このことは、機械的に暗号を解読するコンピュータにおいては大きな問題となる。

【0015】また、IDカードや、キャッシュカードなどでは、カードの磁気記録部分にIDカードにおいてはID番号、キャッシュカードにおいては口座番号が、暗証番号とともに記録されている。これらのカードは、通常、ID番号、口座番号はカード表面に記入されている場合が多い。従って、磁気記録部分が暗号化されている場合には、原文であるID番号、口座番号とそれらに対応する磁気記録部分の暗号文を比較することにより暗号化方式を推定することができる。従って、暗証番号に相当する原文を第三者に解読されてしまう畏れがある。また、磁気記録部分が暗号化されておらず、公開されているコード体系、記録方式を用いている場合でも、ID番号、口座番号とそれらに対応する磁気記録部分を比較することによりどのコード体系、記録方式を使用しているかが第三者にわかつてしまい、暗証番号を読みだすための手掛かりを与えてしまう。

【0016】リモートセンシングデータ、有料の放送内容、コンピュータデータ、IDカードなどにおいて特定の符号パターンの出現頻度が極端に高く、原文のパターンが容易に推定されやすく、暗号が解読されやすい用途での暗号化によるデータ伝送方式を提供することを目的とする。

【0017】

【課題を解決するための手段】上記目的を達成するため本発明では、伝送すべきデータの暗号化は以下のように行われる。

【0018】原文において、出現頻度が高いパターン（符号）のグループと出現頻度が低いパターン（符号）のグループとに分類し、それぞれのグループごとに別々の暗号化方式または、暗号化鍵を用いて暗号化する。

【0019】DPCM方式のリモートセンシングデータの伝送においては、差分0を表す符号と差分0以外を表す符号とを別々の暗号化方式または、暗号化鍵を用いて暗号化する。

【0020】有料の衛星放送などの加入放送では、テストパターンの画像と通常の放送番組とで別々の暗号化方式または、暗号化鍵を用いて暗号化（スクランブリング）する。

【0021】コンピュータで扱うデータの伝送においては出現頻度の高い\$00や\$FF、そしてNOP（Non Operation）命令に相当する符号と、それ以外の符号とを別々の暗号化方式または、暗号化鍵を用いて暗号化する。

【0022】IDカードや、キャッシングカードなどにおいては、ID番号、口座番号と暗証番号とを別々の暗号化方式または暗号化鍵を用いて暗号化する。

【0023】

【作用】本発明によれば、原文において、出現頻度が高いパターン（符号）のグループと低いパターン（符号）のグループとに分類しているために、それぞれのグループ毎に別々の暗号化方式または、暗号化鍵を用いて暗号化するため、出現頻度が高いパターン（符号）のグループが手がかりになって、出現頻度が低いパターン（符号）のグループの暗号が解読されることがない。

【0024】またDPCM方式のリモートセンシングデータの伝送においては、差分0以外のデータが重要であり、本発明によれば差分0を表すデータの出現頻度が高いという事前の知識から、差分0以外を表すデータに相当する暗号文を第三者に解読される畏れが少なくなる。

【0025】一方、有料の衛星放送では、テストパターンの画像の持つ規則性から、通常の放送番組のスクランブリングを第三者に解読される畏れが少なくなる。

【0026】またコンピュータで扱うデータの伝送においては、原文中の\$00や\$FF、そしてNOP命令に相当する符号の出現頻度が高いという知識からそれ以外の符号に相当する暗号文が第三者に解読される畏れが少

なくなる。

【0027】更にIDカードや、キャッシュカードなどにおいては、カードに記載されているID番号、口座番号を手掛かりに暗証番号に相当する暗号が第三者に解読される畏れが少なくなる。

【0028】

【実施例】以下、本発明の実施例を図面を参照して説明する。

【0029】図1には本発明に係る暗号化データの伝送方法の原理が示されている。同図において原文1の符号、文字、データは出現頻度に応じて、出現頻度の高い符号、文字、データはグループAに、出現頻度の低い符号、文字、データはグループBに分類される。グループAに分類された符号、文字、データはグループAに対応したKAなる暗号化方式または、暗号化鍵を用いる暗号化操作10により暗号化され、グループBに分類された符号、文字、データはグループBに対応したKBなる暗号化方式または、暗号化鍵を用いる暗号化操作11により暗号化され暗号文2が得られる。この暗号文2が送信側から受信側へ種々の伝送手段により送信される。

【0030】一方、暗号文の受信側では、それぞれのグループに対応した暗号解読操作20、21で暗号を解読し、原文3を得ることができる。出現頻度が高い符号、文字、データの集合体であるグループAの暗号は解読されやすい。しかし、本実施例によれば、グループBの暗号はグループAとは別個の暗号化方式、または暗号化鍵を用いているので解読されにくい。

【0031】また極端な場合、グループAの原文の内容は第三者に知られても構わない場合には、グループAの原文は暗号化せず、グループBの原文のみ暗号化することも有効である。

【0032】図2、図3には、本発明に係る暗号化データの伝送方法における原文のグループ判別的方式が示されている。図2に示すようにグループAに属する原文はKAなる暗号化方式または、暗号化鍵を用いる暗号化操作10により暗号化され、グループBに属する原文はKBなる暗号化方式または、暗号化鍵を用いる暗号化操作*

$$C = K \text{ eor } x$$

但し、C : 暗号

K : 暗号化鍵

x : 原文

eor : 排他的論理和演算子

$$Ca = KA \text{ eor } xa$$

$$Cb = KB \text{ eor } xb$$

サブグループa、bに属する原文xa、xbは暗号化鍵★

$$KA \text{ eor } xa = KB \text{ eor } xb$$

$$\therefore xb = KB \text{ eor } KA \text{ eor } xa$$

である。ここで、サブグループbに属する原文xbは暗号化鍵★

$$Cb' = KX \text{ eor } xb$$

ここで、Cb'が他の暗号化鍵による暗号と識別が可能

* 11により暗号化される。

【0033】上記のように暗号化するとグループBのうちサブグループbとグループAのうちサブグループaが同じ暗号文に暗号化される場合がある。すると、暗号の受信側では、暗号文の符号がグループAに属するもののかグループBに属するもののか判別できない。コンピュータを用いて暗号化、暗号解読を行う場合には、ヒューリスティックス（直感的知識）を使用できないために、暗号文と原文とは一義的に対応しなければならない。

10 このような場合には、図3に示すようにグループ判別手段40の結果41を暗号の受信側にも送ればよい。図3において、グループ判別結果41に基づきスイッチ30、31、32、33を切り替えてグループごとに適した暗号化方式または、暗号化鍵を選択して暗号化及び、暗号解読を行う。

【0034】図4にはグループ判別手段40の具体的構成が示されている。同図においてグループAに属するパターン群42-1～42-Nと原文1のパターンとが比較手段43-1～43-Nで比較され、原文1がグループAに属するパターン群42-1～42-Nのいずれかと一致した場合には原文1のパターンがグループAに属すると判定され、オアゲート44を介して判別結果41が出力される。

【0035】次に図5、図6に図2、図3に示す実施例においてグループ判別結果41を暗号の送信側から受信側へ送る必要をなくした実施例を示す。これらの図において暗号化方式または、暗号化鍵KBを用いる暗号化操作11によってサブグループaと同じ暗号に暗号化されるサブグループbをKBとは異なる暗号化方式または、暗号化鍵KXを用いる暗号化操作12で暗号化することによってサブグループaと同じ暗号に暗号化されることを防止している。

【0036】暗号化方式または、暗号化鍵KXの定め方は、暗号化方式または、暗号化鍵KA、KBによって異なる。たとえば式(1)のように排他的論理和(exclusive-or)により暗号化する場合を考える

..... (1)

※図2においてサブグループa、bに属する原文xa、xbは暗号化鍵KA、KBにより以下のように暗号Ca、Cbに変換される。

【0037】

..... (2)

..... (3)

★KA、KBにより同一の暗号に変換されるから、

..... (4)

..... (4')

★号化鍵KXにより暗号Cb'に暗号化されるから、

..... (5)

であるためには、

$C b' \neq \{CA : CA=KA \text{ eor } x A\}$ かつ、
 $C b' \neq \{CB : CB=KB \text{ eor } x B\}$

10 (6)

となるように暗号化鍵K Xを選べばよい。ここで $x A$ は
グループAに属する原文、 $x B$ はグループBに属する原
文であり、 \neq は \in の否定、すなわち「属さない」こと*

$K X=KA$

..... (7)

とおくと、

$C b' = KA \text{ eor } x b \neq \{CA : CA=KA \text{ eor } x A\}$

また、 $KA \text{ eor } KA=0$ であるから、式(4')より

$C b' = KB \text{ eor } x b \neq \{CB : CB=KB \text{ eor } x B\}$

となり、暗号化鍵K Xは式(6)の条件を満たすことが
できる。

【0039】次に図7を参照して具体的なデータを例に
して説明する。同図において、\$FF (2進数で 1111
1111)、\$00 (2進数で 0000 0000)をグループAに
属する原文と仮定し、それ以外のデータをグループBとす
る。また、暗号化鍵KA、KBをそれぞれ\$AA (2進
数で 1010 1010)、\$99 (2進数で 1001 1001)と仮
定する。

【0040】グループAに属する原文\$FF、\$00は暗
号化鍵KAとのピットごとの排他的論理和演算によつて
図7に示すように暗号\$AA (2進数で 1010 1010)、
\$55 (2進数で 0101 0101)に変換される。

【0041】一方、暗号化鍵KBによって暗号\$AA、
\$55に変換される符号すなわちサブグループbに属す
る符号は、それぞれ\$33 (2進数で 0011 0011)、\$
CC (2進数で 1100 1100)である。従つてサブグル
ープbに属する符号\$33、\$CCは暗号化鍵KAによつて
それぞれ暗号\$66 (2進数で 0110 0110)、\$99
(2進数で 1001 1001)に変換される。

【0042】暗号の受信側では、暗号\$AA、\$55、
\$66、\$99が来たら、暗号化鍵KAを用いて暗号を
解読し、それ以外の暗号が来たら暗号化鍵KB用いて暗
号を解読すれば、原文を得ることができる。

【0043】本実施例によれば、グループ判別結果を受
信側に送る必要がなくなるので、伝送する情報量が少
なくてすむほか、第3者に暗号解読のヒントを与える機会
も少なくなる。

【0044】図8には、図5、図6に示した実施例にお
ける暗号化鍵KA、KBが固定パターン（時系列的に変
化しないパターン）である場合のグループ判別手段40
Aの具体的構成が示されている。暗号化鍵が固定パ
ターンである場合には、グループAに属するパターン群42
-1～42-Nが判れば、サブグループbに属するパ
ターン群44-1～44-Nも固定パターンとして予め決
定できるため、以下のように原文1と固定パターンとを
比較することにより原文のグループ判別が可能となる。

【0045】まずグループAに属するパターン群42-
1～42-Nと原文1のパターンとが比較手段43-1
～43-Nで比較され、原文1がグループAに属するパ
50

*を表している。

【0038】

..... (7)

ターン群42-1～42-Nのいずれかと一致した場合
には原文1のパターンがグループAに属する判定され、
オアゲート50-1を介して判別結果41 (41A) が
出力される。

【0046】次にサブグループbに属するパターン群4
4-1～44-Nと原文1のパターンとが比較器群45
-1～45-Nで比較され、原文1がサブグループbに
属するパターン群44-1～44-Nのいずれかと一致
した場合には原文1のパターンがサブグループbに属す
ると判定され、オアゲート50-2を介して判別結果4
1 (41B) が出力される。

【0047】また、上記(1)にも(2)にも該当しな
い場合には原文1のパターンがサブグループbを含ま
ないグループBに属すると判定され、オアゲート50-
2、アンドゲート51を介して判別結果41 (41C)
が出力される。

【0048】図9は、図5、図6に示した実施例にお
ける暗号化鍵KA、KBが固定パターンである場合のグル
ープ判別手段40Bの実施例である。この場合もグル
ープAに属する暗号のパターン群46-1～46-Nが判
れば、サブグループbに属する暗号のパターン群48-
1～48-Nも固定パターンとして予め決定できるた
め、以下のように原文1の暗号文2と固定パターンとを
比較することにより暗号文のグループ判別が可能とな
る。

【0049】まずグループAに属する暗号のパターン群
46-1～46-Nと暗号文2のパターンとが比較手段
47-1～47-Nで比較され、暗号文2がグループA
に属する暗号のパターン群46-1～46-Nのいずれ
かと一致した場合には暗号文2のパターンがグループA
に属する暗号と判定され、オアゲート60-1を介して
判別結果62 (62A) が出力される。

【0050】次にサブグループbに属する暗号のパ
ターン群48-1～48-Nと暗号文2のパターンとが比較
手段49-1～49-Nで比較され、暗号文2がサブグ
ループbに属する暗号のパターン群48-1～48-N
のいずれかと一致した場合には暗号文2のパターンがサ
ブグループbに属する暗号と判定され、オアゲート60
-2を介して判別結果62 (62B) が出力される。

【0051】また、暗号文2がパターン群46-1～4

6-N、あるいはパターン群48-1~48-Nのいずれにも一致しない場合にはオアゲート60-1, 60-2及びアンドゲート61により暗号文2のパターンがサブグループbの暗号を含まないグループBに属すると判定され、判別結果62(62C)が出力される。

【0052】また、暗号化鍵KA, KBが固定パターンでなく、シフトレジスタなどを用いて生成されたM系列などの乱数である場合には、サブグループbに属するパターン群44-1~44-Nは、図10に示すようにグループAに属するパターン群42-1~42-N及び、暗号化鍵KA, KBによって決定される。

【0053】この場合、サブグループbに属する暗号のパターン群48-1~48-Nは、図11に示すようにサブグループ(b)に属するパターン群44-1~44-N及び、暗号化鍵KXによって決定される。

【0054】なお以下に示す実施例では、簡単のために図2、図3に示した実施例の応用例について説明を加えるが、図5、図6に示した実施例も適用可能であることは勿論のことである。

【0055】図12、図13には遠隔地の計測点100での計測データをDPCM方式により圧縮して遠隔地の処理センタ101へ伝送する暗号化データ伝送方式の実施例が示されている。図13に示すように差分0に相当する符号をKAなる暗号化方式または、暗号化鍵を用いた暗号化操作10により暗号化し、差分0以外の値に相当する符号をKBなる暗号化方式または、暗号化鍵を用いた暗号化操作11により暗号化して、暗号文2を得る。得られた暗号文2は公衆通信回線などの種々の伝送手段により受信側に伝送される。暗号文の受信側では、それぞれのグループに対応した暗号解読操作20, 21で暗号を解読し、原文を得ることができる。

【0056】本実施例によれば、差分0のDPCM符号の出現頻度が高いという知識から差分0以外の値を表すDPCM符号の解読の手掛かりを第三者に与える畏れがなくなる。

【0057】次に図14、図15に本発明を加入放送のスクランプリングに適用した実施例を示す。これらの図において放送事業者102では、加入者以外が放送を聴取するのを防ぐために、放送内容を暗号化(スクランプリング)して、無線又は有線により加入者103へ放送内容を送る。加入者103では、放送事業者より配布されたデコーダにより暗号(スクランプリング)を解読して放送を聴取することができる。本実施例では、図15に示すようにテストパターンをKAなる暗号化方式または、暗号化鍵による暗号化操作10により暗号化(スクランプリング)し、通常の放送をKBなる暗号化方式または、暗号化鍵による暗号化操作11により暗号化(スクランプリング)して、暗号文2を得る。得られた暗号文2は無線や有線などの種々の伝送手段により受信側に伝送される。暗号文の受信側では、それぞれのグループ

に対応した暗号解読操作20, 21で暗号文を解読し、原文を得ることができる。

【0058】本実施例によれば、テストパターンの持つ規則性を手がかりにして、KAなる暗号化方式または、暗号化鍵による暗号化操作10によるスクランプリングが第三者に解読されても、KBなる暗号化方式または、暗号化鍵を用いた暗号化操作11によるスクランプリングが解読されるのを防ぐことができる。

【0059】図16、図17にはコンピュータ104を遠隔地にある保守センタ105から遠隔保守する場合に本発明が適用された実施例が示されている。コンピュータを遠隔保守する際には保守センタ105からコンピュータ104にプログラムを転送したり、コンピュータ104内のデータをコンピュータ104から保守センタ105へ転送したりする。この際に、コンピュータで扱うデータのうち\$00, \$FFのデータやNOPを表す機械語コードをKAなる暗号化方式または、暗号化鍵による暗号化操作10により暗号化し、それ以外のデータをKBなる暗号化方式または、暗号化鍵による暗号化操作11により暗号化して、暗号文2を得る。得られた暗号文2は無線や有線などの種々の伝送手段により受信側へ伝送される。暗号文2の受信側では、それぞれのグループに対応した暗号解読操作20, 21で暗号文2を解読し、原文3を得ることができる。

【0060】図18は、図16、図17に示す実施例における暗号化の具体例である。

【0061】原文“\$0000FFF1234”(2進数で0000 0000 0000 11111111 1111 1111 0001 0010 0011 0100)を暗号化鍵“\$AA”(2進数で10101010)との8ビットをブロックとしたビットごとの排他的論理和(exclusive or)を探る従来の方法で暗号化すると暗号文“\$AAAA5555B89E”(2進数で1010 1010 1010 1010 0101 0101 0101 0101 1101 100 1001 1110)が得られる。

【0062】また、原文“\$FF”(2進数で1111 1111)及び、“\$00”(2進数で0000 0000)を暗号化鍵“\$AA”、それ以外の原文を暗号化鍵“\$99”(2進数で1001 1001)との8ビットをブロックとしたビットごとの排他的論理和(exclusive or)を探る本発明の方法で暗号化すると暗号文“\$AAAA55558BAD”(2進数で1010 1010 1010 1010 0101 0101 0101 0101 0101 1000 1011 1010 1101)が得られる。

【0063】従来の方法では、コンピュータデータ中(原文中)の“\$FF”及び、“\$00”的出現頻度が高いという知識から暗号文中で出現頻度の高い“\$AA”, “\$55”が原文“\$FF”, “\$00”に対応する暗号であることが判る。従って暗号化鍵は“\$AA”または“\$55”的いずれかであることが判る。従って暗号文“\$B89E”に対応する原文は、“\$1234”または、“\$8DCB”(2進数で1000 1101 1110 0000)である。

100 1011) であると推定できる。

【0064】しかし、本発明の方法によると、コンピュータデータ中(原文中)の“\$FF”及び、“\$00”の出現頻度が高いという知識から暗号文中で出現頻度の高い“\$AA”、“\$55”が原文“\$FF”、“\$00”に対応する暗号であることが判り、暗号化鍵は“\$AA”または“\$55”的いずれかであることが判っても暗号文“\$8BAD”はまったく異なる暗号化鍵で暗号化されているために、上記の知識から原文を推定することはできない。

【0065】本実施例によれば、コンピュータデータの出現度数分布を手がかりにして、KAなる暗号化方式または、暗号化鍵を用いた暗号化操作10による暗号文が第三者に解読されても、KBなる暗号化方式または、暗号化鍵を用いた暗号化操作11による暗号文が解読されるのを防ぐことができる。

【0066】図19、図20にはIDカードやキャッシュカードに本発明が適用された実施例が示されている。これらのカード106の磁気記録部分107にはID番号、口座番号とともに正当な使用者であることを認証するために、暗証番号が記録されている場合が多い。この場合、ID番号、口座番号(原文)1をKAなる暗号化方式または、暗号化鍵による暗号化操作10により暗号化し、暗証番号をKBなる暗号化方式または、暗号化鍵を用いた暗号化操作11により暗号化して、暗号文2を得る。得られた暗号文2は磁気記録手段などによりカード106に記録される。カード読み取り機では、それぞれのグループに対応した暗号解読操作20、21で暗号文2を解読し、原文3を得て、正当な使用者であるかどうかを判断する。

【0067】本実施例によれば、カード106表面に記載されているID番号、口座番号を手がかりにして、KAなる暗号化方式または、暗号化鍵を用いた暗号化操作10による暗号文が第三者に解読されても、暗証番号のKBなる暗号化方式または、暗号化鍵を用いた暗号化操作11による暗号文が解読されるのを防ぐことができる。

【0068】また暗号化しないまでも、一般に公開されているコード体系、記録方式を用いる場合でも、ID番号、口座番号と暗証番号を別個のコード体系、記録方式により記録すれば、同様の効果が得られる。例えば、ID番号、口座番号をアスキーコードで記録し、暗証番号を二進化十進(BCD)コードで記録する方法とか、ID番号、口座番号と暗証番号を異なるアジマス角で記録するなどの方法が考えられる。

【0069】以上本発明の実施例について説明したが、本発明を従来の暗号化方式と組み合わせて用いると更に暗号強度が増すことはもちろんのことである。例えば、本発明による暗号化を実施したのちにDES暗号による暗号化を施せば、コンピュータデータ伝送に最適な暗号

化によるデータ伝送方式を提供することができる。

【0070】

【発明の効果】本発明によれば、原文を構成する文字、符号、データの種別に応じて複数の暗号化方式または暗号化鍵を使い分けるようにしたので、原文中の符号の出現頻度に関する知識や、原文の推定を手がかりにして、暗号が第三者に解読される畏れを少なくすることができる。

【図面の簡単な説明】

10 【図1】本発明に係る暗号化データの伝送方法の基本的原理を示す説明図である。

【図2】本発明に係る暗号化データの伝送方法の一実施例を示す説明図である。

【図3】本発明に係る暗号化データの伝送方法の一実施例を示す説明図である。

【図4】図3におけるグループ判別手段の具体的構成を示すプロック図である。

【図5】本発明に係る暗号化データの伝送方法の他の実施例を示す説明図である。

【図6】本発明に係る暗号化データの伝送方法の他の実施例を示す説明図である。

【図7】データの暗号化の具体例を示す説明図である。

【図8】図6におけるグループの判別手段40Aの具体的構成を示す説明図である。

【図9】図6におけるグループ判別手段40Bの具体的構成を示す説明図である。

【図10】暗号化鍵が固定パターンでない場合における暗号化の過程を示す説明図である。

【図11】暗号化鍵が固定パターンでない場合における暗号化の過程を示す説明図である。

【図12】本発明が適用されるリモートセンシングシステムを概念的に示す説明図である。

【図13】本発明が適用されるリモートセンシングシステムにおける暗号化データの伝送方法の実施例を示す説明図である。

【図14】本発明が適用される加入放送システムを概念的に示す説明図である。

【図15】本発明が適用される加入放送システムにおける暗号化データの伝送方法の実施例を示す説明図である。

【図16】本発明が適用されるコンピュータの遠隔保守システムを概念的に示した説明図である。

【図17】本発明が適用されるコンピュータの遠隔保守システムにおける暗号化データの伝送方法の実施例を示す説明図である。

【図18】図17におけるデータの暗号化の具体例を示す説明図である。

【図19】本発明が適用されるIDカードの外観を示す説明図である。

【図20】本発明が適用されるIDカードを用いた暗号

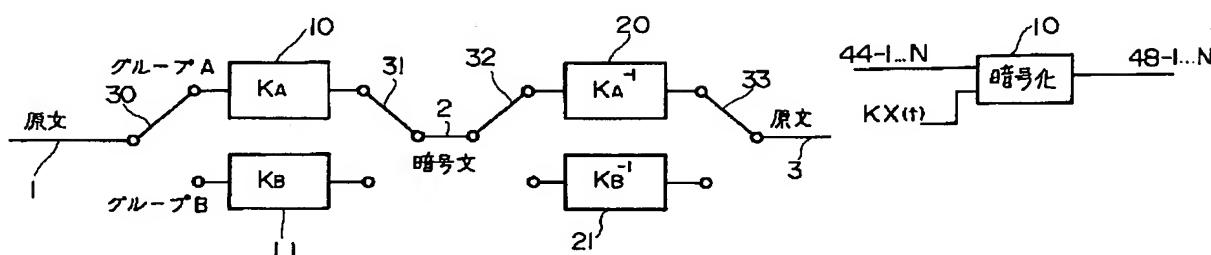
化データの伝送方法の実施例を示す説明図である。

【符号の説明】

- 1, 3 原文
- 2 暗号文
- 10～12 暗号化操作
- 20～22 暗号解読操作
- 30～33 スイッチ
- 40, 40A, 40B グループ判別手段

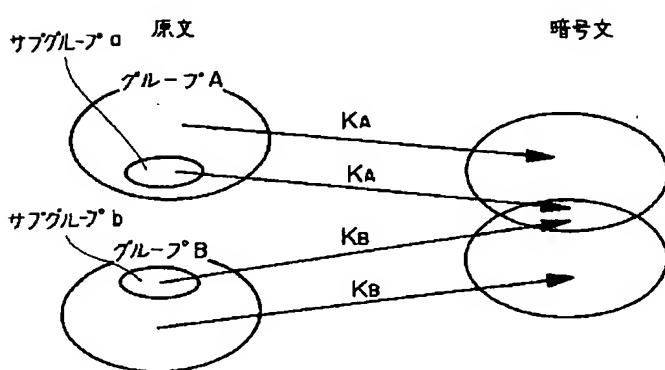
| | |
|-------------|--------|
| * 43-1～43-N | 比較器群 |
| 45-1～45-N | 比較器群 |
| 47-1～47-N | 比較器群 |
| 49-1～49-N | 比較器群 |
| 50-1, 50-2 | オアゲート |
| 60-1, 60-2 | オアゲート |
| 51, 61 | アンドゲート |

【図1】

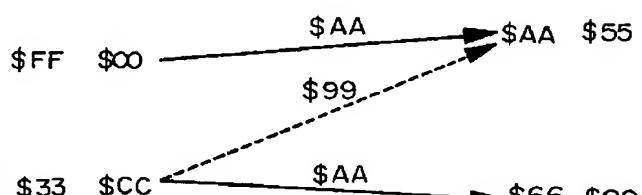


【図11】

【図2】

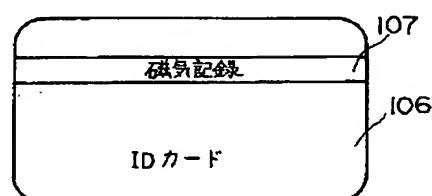
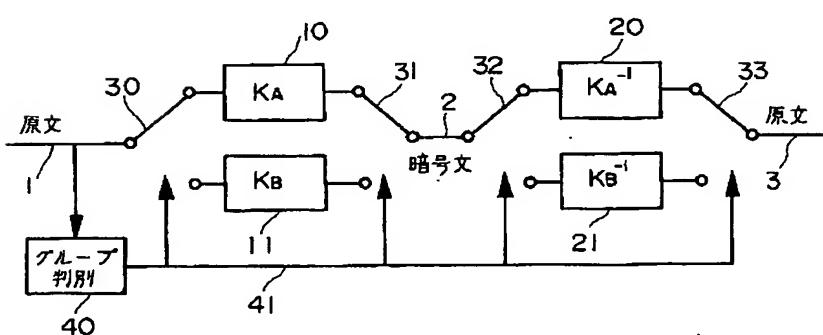


【図7】

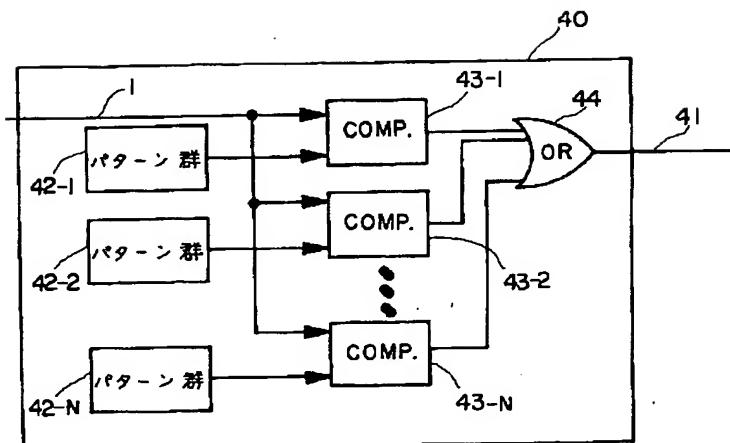


【図19】

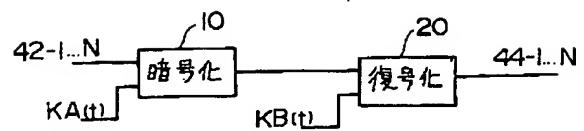
【図3】



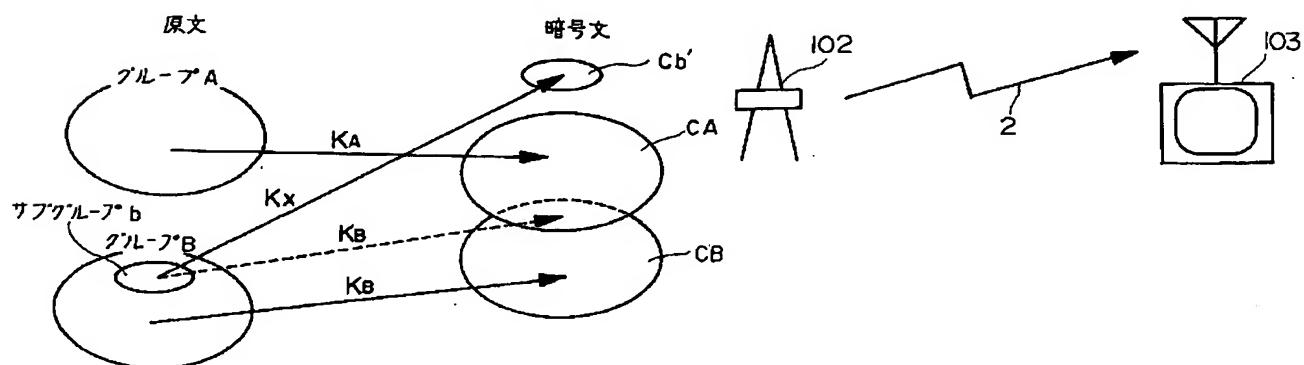
【図4】



【図10】

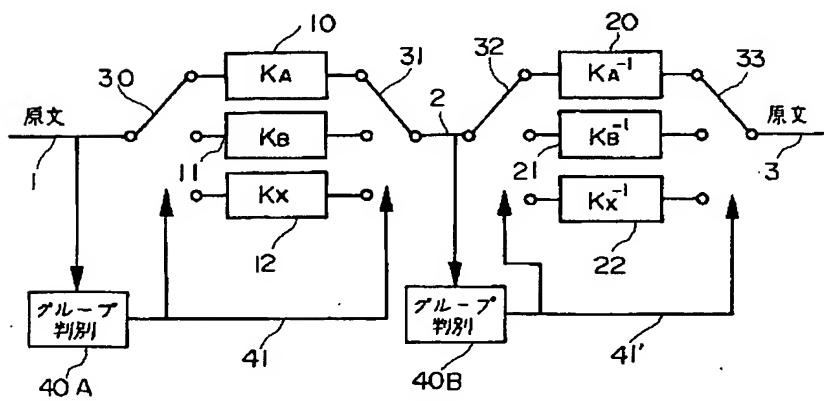


【図5】

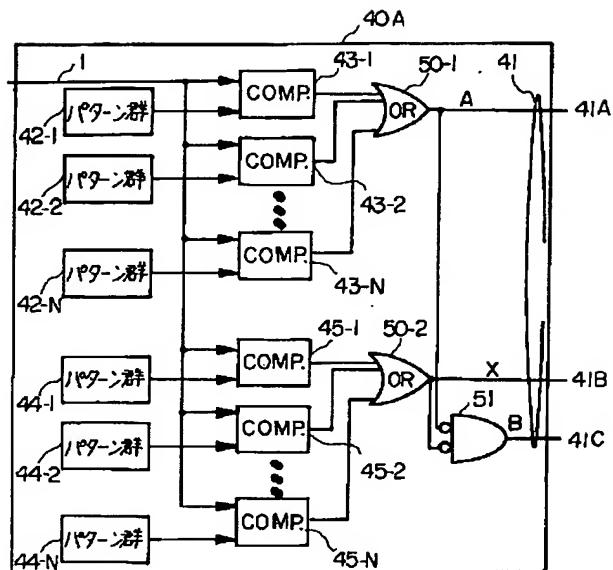


【図14】

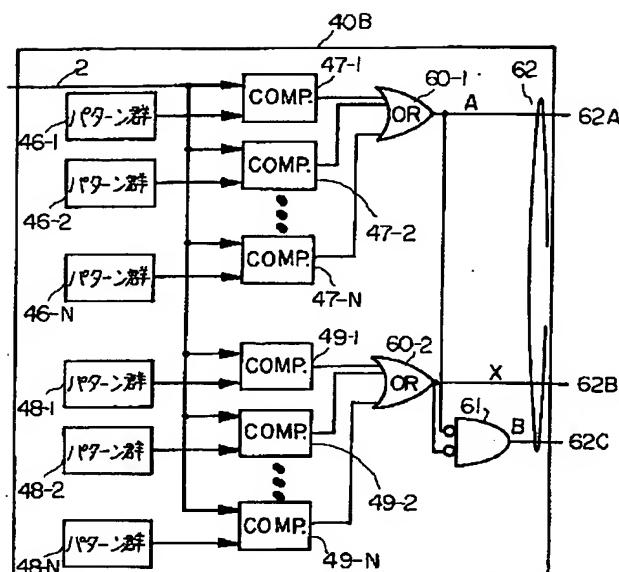
【図6】



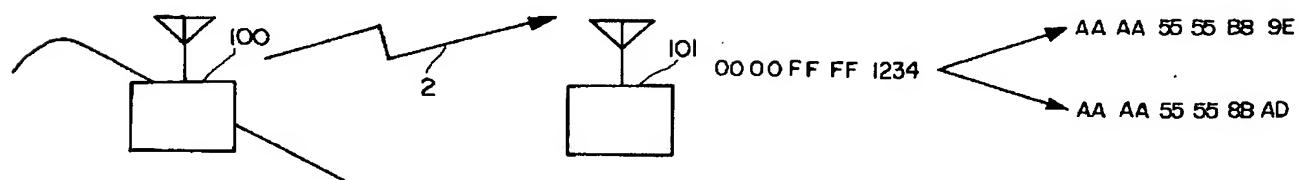
【図8】



【図9】

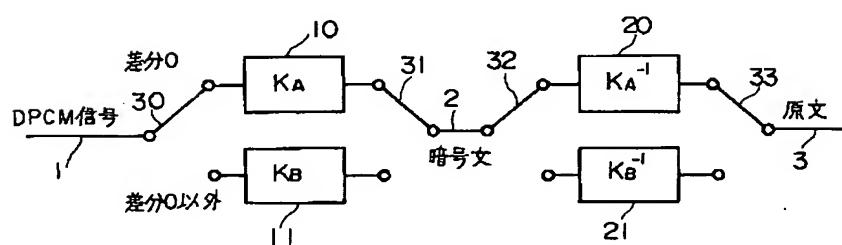


【図12】

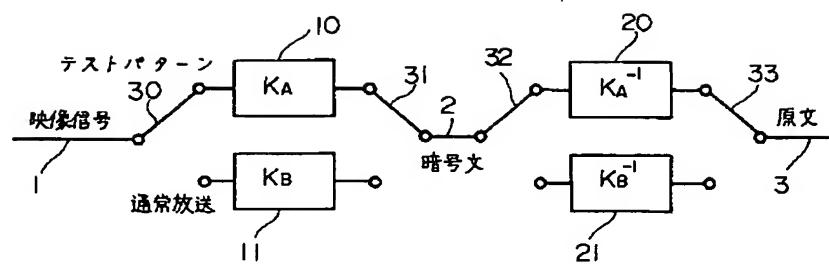


【図18】

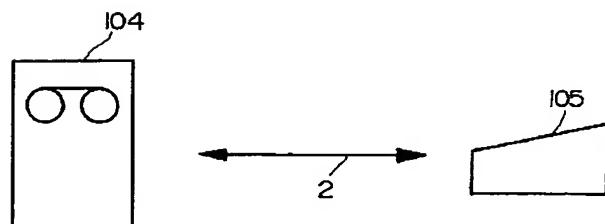
【図13】



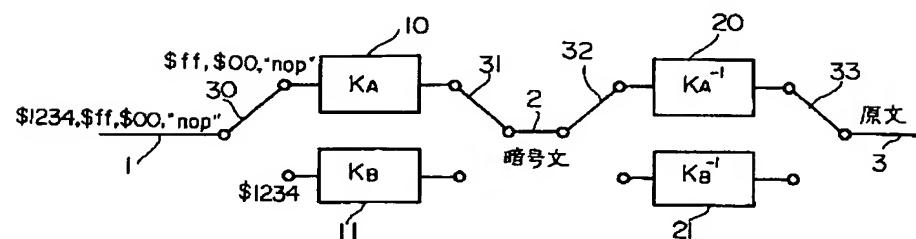
【図15】



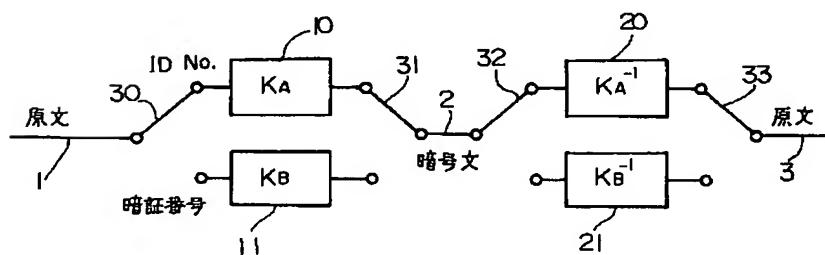
【図16】



【図17】



【図20】



フロントページの続き

| | | | | |
|---------------------------|------|-----------|-----|--------|
| (51) Int.Cl. ⁵ | 識別記号 | 府内整理番号 | F I | 技術表示箇所 |
| G 0 9 C | 1/00 | 9194-5L | | |
| H 0 4 K | 1/00 | Z 7117-5K | | |